Scenario Development in Oil and Gas Management: "Envisioning the Future" by Means of Analytical Techniques

Strategic Insights, Volume VII, Issue 1 (February 2008)

by James David Ballard, Ph.D. and Fred C. Dilger, Ph.D.

Introduction

This paper seeks to derive insight from the rapidly evolving field of hazard mitigation planning to the problem of physical security planning for oil and petroleum facilities. While a number of different approaches to performing security and risk assessments have been used by the industry, none of these singularly or in tandem cohere as a formal physical security process. This paper argues that physical security planning for the oil and gas industry belongs inside a business planning process and should be an ongoing part of business decision-making. We title this the "envisioning the future" model of analysis.

The problems of terrorism and physical security are akin to those of hazard mitigation planning. Conceptually, both result in substantial financial losses as well as a potential for loss of life. They also can result in nonstandard impacts, such as the stigma resulting from an oil spill or a reappraisal of investment risk due to terrorist attack. A critical component that is different in this approach and from the traditional hazard mitigation approach is an underlying belief that it is necessary to integrate a wider array of social scientific data, methods, and concepts into the planning process than in either traditional physical security planning or hazard mitigation planning. This is because petroleum production facilities represent a vital strategic economic and social resource.

The analysis techniques recommended in this paper build on both traditional hazard mitigation and on long standing methods developed by industry leaders. For example the "envisioning the future" paradigm incorporates the latest techniques from 'futurist' researchers to better understand how the risk of a 'worst case' can be managed, (Burby 1998; Glenn and Gordon 1999). The possibilistic analysis used herein moves beyond probabilistic analysis typically used by quantitative risk analysts (Willis, Morral, Kelly and Medby 2005) and into the much needed security arena of identifying and then proactively managing hard to predict risks like those posed by terrorism attacks.

Concept

As noted, the "envisioning the future" method advocates the development and application of a process internal to an organization's business planning process. This method deliberately integrates physical security and business planning systems. In many organizations, physical

security planning is produced outside the mainstream of traditional business planning processes, in many cases as a cost of operations not considered a benefit for the organization.

As a consequence of this disjunction, security plans are not usually tied to business alternatives, what would be the optimal integration strategy. In traditional hazard mitigation planning, this disjunction is referred to as “the window of opportunity". This window occurs in the aftermath of an accident when support by almost everyone for better mitigation planning is at its highest. This broad based support enables the organization to obtain funds for mitigation planning. In some cases it allows for draconian measures that may be needed to ensure the hazard or threat does not occur again. But there are drawbacks with this kind of planning approach. For example, the sense of crisis that is generated creates support for this kind of planning, but it also leads to a tendency to only plan for the most recent problem. Many organizations wind up planning to fight the last war or meet the last threat. They do not fully engage the full range of developing threats; they do not envision a future wherein new threats emerge, threats that can profoundly alter the business model of the industry.

An applicable example of this kind of backward looking planning is found in the United States airline industry. The physical security procedures developed for the U.S. airline industry and used for decades in the industry were in response to isolated hijacking attempts in the 1970s. These long standing procedures were not prepared to deal with the threat that developed in the late 1990’s from terrorism and most vividly manifest in the attacks of 9/11/2001.

The envisioning the future paradigm argues that it is necessary to incorporate physical security and mitigation planning into the business planning process to face these threats. A key part of the process is to effectively use futures techniques to identify and define the problem. That is using the envisioning techniques to find the threats before they occur, not after.

To help illustrate this process, scenarios are developed. These scenarios are not just proxies for threats; properly constructed they can provide vivid descriptions of future circumstances. They can provide specific insight permitting industry managers to prepare for the futures, be it rosy or troubling.

A meta analysis of how scenario planning is typically done shows that the process is driven by probabilistic methods that may overlook the motivations of potential aggressors. Motivations like religion, vengeance and tribal loyalty are powerful forces that are easy to overlook because they are hard to quantify. To help understand this, the paper looks at the history of the oil industry and terrorism to help situation knowledge that needs to be known before planning occurs. The history of attacks on oil production can reveal some of the past trends, but future threats may come from other directions.

Background: Physical Security of Oil

When one considers the vulnerability of the oil and gas infrastructure to any form of terrorism attacks (Adams 2003; Ness 2006), the most obvious way of visualizing these risks would be from a historical perspective. The oil and gas industry has been subjected to attacks over the last 150 years. This history allows scenario developers the chance to anticipate patterns that may reemerge and plan security accordingly.

From its initial industrialization, the production and refining of oil, as well as the facilities used to distribute the final products, have been targeted for violent disruption by a variety of groups. Disruption of oil production has occurred for a multiplicity of reasons and through a diversity of means, but the trend in these attacks is clear. Oil’s hundred year old place as a critical make it a target for human initiated events like terrorism, sabotage, violent political protests and even the

deliberate attempt to halt the processes of oil location, extraction, refining and delivery (Yergin 1992; Yetiv 2004; Kalicki and Goldwyn 2005; Perry 2007)

The first commercial oil well was drilled in Titusville, Pennsylvania (1857). Within six months the sleepy Pennsylvania countryside was transformed into a boomtown of prospective oil men desperate to acquire a secure flow of the "new light." Problems arose immediately, as thousands of people flocked to the area in and around the oil field. As more and more oil wells were discovered, new problems for the burgeoning industry arose—problems with moving the oil from the wells to the processing and distribution center in Philadelphia. By 1863, drillers fed up with exorbitant drayage fees charged to haul their oil to market began the construction of a pipeline. The teamsters who ran the wagon transport operations, who saw their monopoly threatened, counterattacked with threats, armed violence, arson and sabotage (Yergin 1992) . The motive of the attacks was to ensure continued use of horse transport for the oil. Thus the insider/outsider threat was one of the first encountered by the industry.

The use of "new light" changed the world's economy and touched off a scramble for oil that pushed oil industry explorers into ever more distant corners of the globe. After a series of false starts, the Shell Oil Company located a substantial oil field in Sumatra in 1892. Conditions in the developing oil field were horrific. Attacks by local pirates against the oil production facilities compounded the problems of industrializing such an isolated location. The attacks were distinctly low-tech, primarily by means of arson, theft and threats against communications lines. Here the outsider threat to extraction of oil was the primary risk.

In Baku, Southern Russia, labor unrest fermented by communist and local ethnic factions, disrupted oil production from 1903-1905. Strikes and armed insurrection against the oil companies created the first major disruption of oil productions. The Baku strife began with internal labor disputes which had an ethnic component. While labor problems may have originated the problem, the ethnic component of the violence rapidly became the locus of the social problem faced by the industry and resulted in the slaughter of the many Armenians in the area. His struggle was also the training ground for the revolutionaries who would later lead the Russian Revolution. One particularly active participant in the violence was Joseph Stalin who credited this violence for much of his training. Thus, internal threats to the industry became political threats (Yergin 1992) .

Similarly in Persia 1900-1907, local tribes disrupted oil production by extorting tribute from the oil companies trying to develop resources. The production was not seriously disrupted but it did add to production costs and reflected the growing trend toward "baksheesh" or bribes paid by oil companies to secure their production. This is another type of social/political cost that the oil and gas industry would endure in many parts of the world.

World War I inaugurated the era of oil as a crucial economic and military resource and tied it to political machinations for generations to come. The conversion of the British Navy to oil ships prior to WWI made the British dependent on oil extracted from Persia in order to operate the naval fleet. This pattern was repeated in many countries around the globe.

The Central Powers also needed oil as fuel for factories and for the vital U-boat campaign against shipping. The earliest attempt to disrupt oil production in the war came in 1914. The Turkish Army recruited local tribesmen for sporadic attacks on the Abadan Island refinery in Persia. Although the force used was small and never completely disrupted production, it did lead to some delay in production. This illustrates the vulnerability of the industry to stalling or disruption tactics.

The First World War also saw two substantial efforts aimed at disrupting petroleum supplies. First the Imperial German Navy's aggressive U-boat campaign from 1917-1918 was aimed at all shipping but also substantially disrupted the flow of oil from the United States. Among the

casualties of the submarine campaign was the world's first oil tanker, Royal Shell's Murex vessel. Here the threat is form global forces, not just an internal or external threat. This threat is part of larger social forces that transcend the industry.

During this war the British sent a single man "Empire Jack" Colonel John Norton-Griffiths to Rumania (1916). He was charged with the task of denying Rumania's oil supplies to the oncoming German Army. In a matter of weeks, Empire Jack had marshaled the voluntary efforts of the Rumanian oil workers and burned, bombed, melted and destroyed every piece of the region's oil production capacity (Bridgeland and Morgan 2003). The German Army was able to make some headway in restoring production since after five months effort, some level of production was restored. The Chief of the Imperial General Staff, Erich Ludendorff acknowledged the harm done to the German war effort. At a critical time, the German Air Force was denied fuel and the German Army lost the flexibility provided by motor transportation. In a similar fashion the vulnerability derives from external social forces.

After the First World War, the social problem of who owned the profits from the sale of oil became more important. Oil had been shown to be a strategic resource that was vital for modern economies and war making capacity—thus nation states felt the need to secure this resource for industrialization, strategic purposes and for national interests. Problems arose as oil companies fought with the governments who owned the land in which the oil was buried. The governments needed the companies to extract, refine and distribute the oil, but the companies needed a stable political environment in which to do their business. This tension would play out for decades to come in various ways around the world.

In the 1920s the Mexican government failed in this stability task and anarchy broke out in the country. The Mexican Revolution disrupted supply as oil companies fought with the Mexican government over the rights to the oil. This disruption led to the nationalization of the companies' oil assets and the creation of PEMEX (Santiago 2006). The nationalization of the oil and gas industry in Mexico was the first of its kind and effectively terrorized investors from participating in the Mexican oil industry for years. This would also be a scenario that played out numerous times around the world over the next few decades.

Oil likewise played a vital strategic role in World War II. Denying access and obtaining access to oil supplies was a vital consideration for all sides in this global conflict, regardless of the economic interests of those countries or the industry. The war saw four significant campaigns against oil production and distribution systems. First was the commencement of the German U-Boat campaign against Allied shipping. As in WWI, tankers were a favorite target of U-boat captains. The Allies sustained horrific losses in freighters in the European theater until 1943 when the Allies gained the upper hand against the U-Boats. The U-Boat attacks significantly delayed the onset of the cross-channel invasion and possibly extended the war by six months to a year.

In 1941, there was a replay of the 1918 efforts noted above but this time at Maikop. One of Hitler's major objectives in Operations Barbarossa, the attack on the Soviet Union, was to secure the Caucasus oil fields. Hitler made seizure of the oil fields a top strategic priority of the Barbarossa offensive and complained that his generals didn't understand the strategic aspects of warfare. The Soviets performed extensive preemptive destruction of the facilities in order to prevent the Nazis from using the fields. Despite this, the Germans were able to repair and use some of the oil from the region. However, the all-consuming need for oil production drove the Germans to reach out to seize Stalingrad, a major industrial city and oil refinery. This ill-fated campaign created the circumstances that lead to the destruction of a substantial part of the German Army and left the Germans too thinly spread to hold the Caucasus.

More indirectly, the campaign in North Africa was also an attempt at disrupting and seizing British oil supplies. Rommel's Afrika Korps had as its key target the Suez Canal. Seizure of this canal would have disrupted shipments of petroleum from Persia. Had British resistance collapsed and

the Germans been free to drive into the Middle East at will, they would have opened another front and attacked the Caucasus from the south.

Throughout the war, Hitler was acutely aware of his nation's dependence on oil. In 1943, the Fifth Air Force, on the orders of General Carl Spaatz, shifted its operations away from sporadic attacks on industrial facilities to a concentrated effort to destroy Germany's oil and synthetic fuel production. These attacks devastated the German war effort and removed vital supplies of synthetic fuel (which was 25% of their fuel by that time). Albert Speer characterized the attacks as the worst blow suffered by the Nazis during the war. Evidence of Speer's perspective is strong since by the end of the war, the German Army was relying on foraged oil supplies and German fighter jets did not have the fuel to fly (Yergin 1992).

Meanwhile in the war against Japan, oil was equally critical. A policy of denial of oil to the Japanese was implemented in the summer of 1941 and helped persuade the Japanese government that seizing oil supplies to the south was key to their national security. The oil companies preemptively evacuated some of their families and staff and prepared detailed plans for the destruction of the oil fields in advance of Japanese takeovers.

In Borneo (circa 1942), long-standing plans to deny the oil to the oncoming Japanese Navy were implemented. The oil wells were dynamited, materials thrown down the shafts; unrefined oil was spilled out of storage tanks and burned in the face of the onrushing Japanese. Although the damage was considerable, the Japanese had anticipated this and formed a special corps devoted to restoring the oil production as quickly as possible. Oil production was restored after two years but the Japanese faced a different problem. They could not securely distribute the oil they produced.

Unlike the U.S. forces in Europe, the U.S. Navy immediately saw the significance of oil production in the Pacific war. They began an aggressive and effective submarine campaign against Japanese oil shipping. In the Battle of the Marus Sea, the U.S. Navy significantly reduced the volume of the oil being shipped to the Japanese mainland.

The restrictions on Japanese fuel supplies affected the Japanese Navy's tactical ambitions. For example, during the U.S. invasion of the Philippines, the task force with the Japanese battleship Yamato was forced to turn back because of its lack of fuel. The use of Kamikaze planes to attack U.S. forces who were landing in Okinawa was spurred in great part by the lack of fuel. It was possible to load planes with a minimum of fuel and still carry out devastating suicide attacks. Fuel shortages made the task harder, but also promoted its use. The whole of WWII was an era showing the interrelatedness of oil, politics and strategic advantage.

Social unrest in Iran flared up in 1951. Fueled by the anti-British Mohammed Mossadegh, mobs began appearing in Teheran and the central government was on the verge of collapse. This unrest threatened British access to oil and was the direct outgrowth of ongoing pressure on oil companies to share greater amounts of their profits with the locals from whose land the oil was drawn. In response, under what was termed "Plan Y" the British contemplated seizing or sabotaging the oil refinery at Abadan (*Time* October 8, 1951). This would have effectively cut off oil funds to the Iranian government. The response to this threat eventually evolved into a British embargo of Iran and was resolved when the Shah of Iran retained his authority.

In July 1956 Egypt nationalized the Suez Canal and provoked the Suez crisis. Gamel Nasser ordered his troops to seize the canal and the Tapline oil pipelines. The Suez Canal's primary value at that point was the shipment of oil from the Mideast to Europe. In response to the seizure, Israel, France and Great Britain launched military actions to free the canal and the pipeline. These military actions prompted Nasser to disable the canal by sinking ships in the entrances and destroying Tapline pumping facilities. This sabotage effort was only briefly successful since it

interrupted the flow of oil through the Suez Canal, but it also speeded up the trend toward supertankers and reduced the Suez Canal's strategic importance (Yergin 1992) .

In 1967, during the Six-Day war, the Middle East erupted in strikes, riots, protests and sabotage that disrupted oil production (Mansfeld 1999; Sampson 1975). The war reduced production by six million barrels a day—over 60 percent of production capacity at the time. More serious than the military actions inspiring this loss of production was the oil embargo which followed. This collective social protest action caused the United States to open its own internal supplies in order to prevent economic disruptions in Europe. In this era oil became a tool of protest and economic blackmail.

The Yom Kippur War (1973) led to a rolling production reduction and embargo which increased prices (Toffler 1980; Mansfeld 1999; Chaliand and Blin 2007). It touched off massive economic disruptions in the United States and Western Europe. The effective use of the "oil weapon" demonstrated that the disruption of oil supplies could be a strategic asymmetrical tactic.

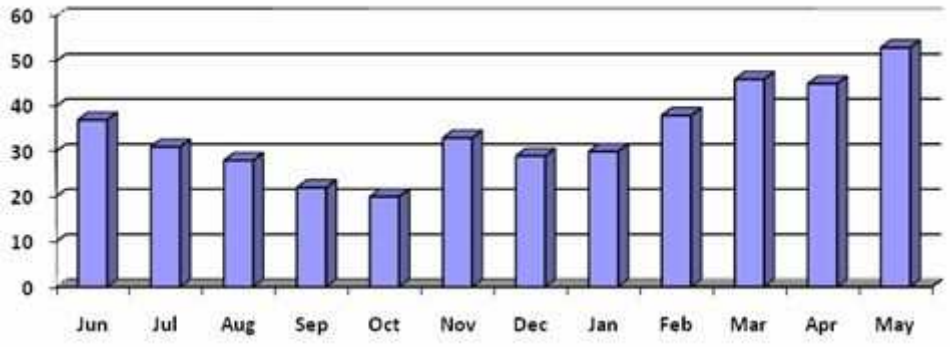
The Iran-Iraq war in 1980 began with Iraqi attacks on Iran's oil production facilities. The original attacks on the Abadan refinery and oil wells in the western portion of Iran were undertaken by Iraqi aircraft and commando squads (Hamilton 1983; Hiro 1991; Alnasrawi 1994). A decade or so later (1991) and in response to the impending defeat of his conventional forces, Saddam Hussein ordered the implementation of his form of environmental terrorism, a plan to spill and destroy as much of Kuwait's oil as possible (Adams 2003). The first 'Gulf' war led to the world's largest oil spill with over six million gallons of crude being released, spilled or burned. The current war in Iraq offers new insight into the physical security of oil facilities.

In summary, history tells us that oil is critical, has been a target and can be used in a wide variety of ways. Knowledge of these can inform policy; especially since the old adage "nothing is new" applies to the industry. New manifestations of terrorist tactics are better understood as variations on themes, some as old as the industry.

Recent Data on Terrorism Attacks

The historic lessons told by the incidents noted above are playing out in the contemporary world. Oil is a target and the industry needs to be proactive in addressing that threat. Recent trends help make this point. In Figure One below the twelve month trend in global oil and gas industry attacks is demonstrated.

Figure One: Global Trends in Oil and Gas Related Terrorism, June 2006 to May 2007



Source: Threat Reduction Limited (2007).

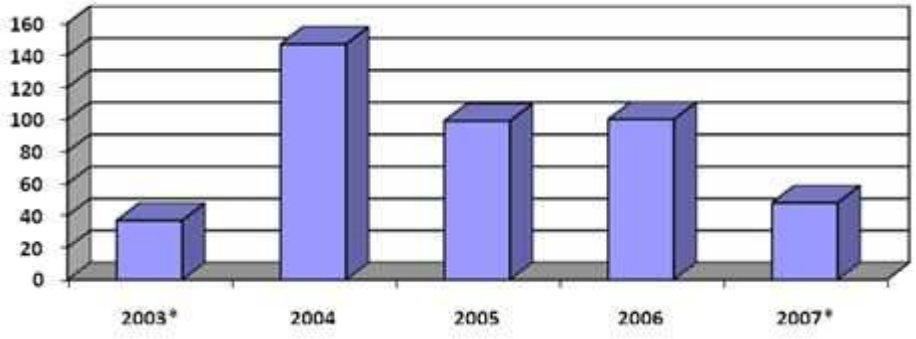
Detailed analysis of this worldwide terrorism attack data shows both infrastructure related (those most obvious to many managers) *and* personnel risks (many times more obscured). For example, during May 2007, twenty-one murders of and twenty-two injuries to oil and gas personnel were recorded. Additionally, fifty-one kidnappings of oil and gas personnel transpired worldwide that month, with twenty-one being released and thirty still held.

The Oil and Gas Industry Terrorism Monitor (Threat Reduction Limited 2007) data that is the basis of Chart One shows that many regions of the world are experiencing such attacks—in fact the following areas around the globe are listed as risk critical—Nigeria, Iraq, Pakistan, India, Afghanistan, and the Russian Federation.

This global phenomenon demonstrates that this is not an isolated threat. Threats from such diverse organizations as Nigerian militants, al-Qaeda, Iraqi insurgents, Taliban, Kurdish Workers Party, United Liberation Front of Assam and others are of note during this time frame. The data suggests that the oil and gas industry faces a worldwide threat and from a variety of motivated adversaries.

In Figure Two the focus is on terrorist attacks that have transpired inside the country of Iraq, one of the most volatile social-political environments in which oil and gas companies conduct business. These in-country attacks were perpetrated against infrastructure like pipelines and oil drilling installations. Once again include attacks against oil related personnel are also noted. The data is for the time frame—June 12, 2003 to May 28, 2007. Please note the data is only partial for the years 2003 and 2007 since the Iraqi specific terrorism data started being collected in mid-2003 and data for the full 2007 year is not yet available.

Figure Two: Iraq Attacks 2003 to 2007



Source: Institute for the Analysis of Global Security (2007)

The contemporary tactics employed by terrorists in Iraq and elsewhere are illustrative of the risks faced by the industry. These include missile attacks that strike oil related facilities, improvised explosive device (IED) attacks on pipelines and against highway tankers, explosive formed projectiles (EFP) attacks on highway tankers and infrastructure, abductions/kidnappings/killings of oil company personnel, railway related attacks and piracy attempts on sea borne vessels.

The wide range of geographic locations, the various groups of motivated attackers who have targeted the oil and gas industry and the variety of tactics they have employed is impressive for its diversity. Such data, coupled with the historical risks noted above, calls into question how the industry will secure itself, its operations, and its personnel in the face of seemingly mounting attention by terrorists towards the oil and gas infrastructure worldwide.

The data and recent research shows that the threat of terrorism against oil and gas infrastructure is critical to understand in order to better mitigate the risks of an attack and the consequences that arise after an attack (Makarenko 2003). In order to tackle the task of envisioning the future such data must be known and factored into planning. The following section will address the ways to organize such data and to plan for the worst case scenarios that should be the basis of safety and security operations.

Human Initiated Events and Worst Case Analysis

Security professionals typically use one or more techniques to assess the risk of 'worst case' attacks against oil and gas infrastructure. These include threat assessments, weapon profiles, risk analysis, security concepts, security audits, consequence analysis, response planning and probable maximum loss studies (PML). These techniques have been adapted from a variety of business sources and primarily address the economic consequences of a potential attack. Thus they represent the cost-benefit paradigm behind much risk assessment and have a rich history of use in this and many industries. They do not necessarily address the need to look at the larger social factors behind the attacks and thus miss important contemporary factors that can become historical facts inflaming risks, factors that are well illustrated by the delineation of historical trends noted above. At the same time these traditional techniques may fail to address emerging threats posed by contemporary terrorists and fail to anticipate new tactics that terrorists may use.

In a similar fashion as the oil and gas industry, safety and security planners in the security sensitive nuclear energy sector have used the design basis threat (DBT) methodology to address the risks posed by terrorism and sabotage (USNRC 2007; IAEA 2007; Blankenship 2002). This method of planning for risks involves the use of a predetermined set of criteria for an attack. These may include an estimate of the most likely number of attackers as well as an opinion of the most likely potential weapons and tactics they will use in an attack against a nuclear power plant (NPP). The benefit of such a 'straw man' methodology is that energy related security forces have something to plan for, a template from which to train their counter forces and a way to predict the seemingly unpredictable. This method does not address the motivation of the attacks, just the nuts and bolts of the tactics.

The DBT method has other serious flaws since it tends to reify what a contemporary threat was (at some time in past) and typically it will not change much over time (Ballard 2002a). This then fails to update threats for on-going risks and underestimates changes in methods, tactics, and motivations of the attackers over time and per social circumstance (Ballard 2002b). For example by neglecting the motive for the attacks, the critical distinction between a political attack (designed to change social conditions) and a suicide attack (designed to inflict maximum damage) will be lost. These two varieties of attacks have very different security responses and require very different planning—a critical risk dimension the DBT methodology fails to address.

Addressing the emerging threats posed by a variety of attacks scenarios, the 'unknowable' risk of terrorism, and the hard to predict attacks themselves are critical. A critical step is to understand the vulnerability of this industry to a variety of terrorist attacks—what we have termed human initiated events. The human initiated events include domains of risk—attacks that originate from within the organization (insider threats), attacks that originate outside of the organization (external threats) and they include external social forces that influence the business environment the organization operates within on a daily basis. Insider threats include attacks to secure jobs, to gain money or otherwise undermine the security in place in the industry. External threats may include attacks meant to garner strategic advantage, attacks that are based on extortion, and/or attacks that provide an income stream to a group. Social Forces may seek control over resources, seek to gain a strategic advantage over another group or nation, and/or could be based on national or ethnic pride.

Figure Three: Domains of Risk Concern

These three threat domains help envision a future that is different form how threats are perceived. They represent risks that can overlap and that are mutually reinforcing. For example, if an employee sells critical insider information about security to an outside force, the symbiosis of these two domains is greater than any single impact from one domain itself. Put another way, the risks for the oil and gas industry rise are considerable in any one of these areas, but with interaction between any combinations of these three domains that risk is amplified.

Figure Three helps visualize these interactions and points attention to the decisive center area—a place where all three of the domains overlap. This is the most critical risk area, one that poses the maximum possible impact (MPI) area for the organization wishing to mitigate risks to their operations. Worst case scenarios and their intellectual equivalent the probable maximum loss study, typically focus on one incidence, one critical aspect for the organization, one dimension and/or one function of the overall organization. They fail in recognizing the interaction effect of such diverse domains and thus they fail in helping to mitigate the risks of future worst case threats.

Human initiated events analysis, coupled with a structured means to develop not just creditable but *impactful* worst case scenarios, are one key to understanding such interactive risks and will yield the MPI scenario necessary to plan for the worst case attacks. Human initiated event recognition allow an organization to lay the foundation for meaningful and impactful scenario development and in the process set the stage for the organization to envision its future prior to one of these critical events. It allows the organization to visualize the MPI for the totality of the organization or for a specific industrial sector therein, or for the industry as a whole given the potential risks contained within the overlapping risks noted. The next section will discuss what is needed to set up this foundation and how human initiated event analysis can feed into scenario

development techniques that can help the industry in articulating scenarios that can better locate, define, and mitigate MPI. In other words, it shows how you can envision the future, a future that poses the greatest threat to your organization.

Managing Hard to Predict Risks

Envisioning the future of terrorist attacks is seen by many in the energy industry, especially the more quantitative NPP operators and associated nuclear regulators, as such a low probability event that there is no need to develop more robust scenarios (Halstead, Ballard and Dilger 2001). We strongly disagree with this assessment. Human initiated event analysis, the actual futurist task of identifying the overlapping relevant domains; this analysis requires thought outside of the norm. It demands a different paradigm than the one that traditionally dominates such energy industry discussions. Such risk blindness is understandable but is no longer tolerable given the terrorist imaginations at work. The analyst need just consider three interrelated domains of liability—political, social and legal—to understand what is at stake (see Chart Four).

Figure Four: Liability Pyramid

The oil and gas industry should and does know better than to neglect such liability domains since they are subject to terrorist attacks on an almost daily basis (see Figure One and Four above) and they are subject to liability concerns in almost every political jurisdiction in the world. Failure to recognize these liability related risks in the face of everyday reality of terrorism is a failure of imagination, not one of a hypothetical 10 -8 probability calculation. It is recognizing that what is needed is MPI (*maximum possibility analysis*), not the well known and misused probability equations that obscure the reality of our changing world threat environment.

Human initiated event analysis then is the process of recognizing the potential for insider threats, outside threats and the triple problem that social forces like extreme political changes and/or associated liability risks pose—it is understanding how these interrelated domains can wrought risk on the oil and gas industry that is not prepared for multifaceted attacks, has not planned for

motivated and complex attacks, and has no effective political/liability related cover in the event they transpire.

The potential political fallout, social problems and long term legal liability of underestimating terrorism threats is one measure of this risk and where the future will meet the bottom line if such planning is not undertaken. That is the greatest justification for integrating management planning and security planning—the bottom line will be hurt if this is not done. All of us who work in the energy industry can envision that future—but can we envision one where we mitigate those risks?

The Planning Process

This paper proposes using a hazard mitigation model for identifying physical security requirements for oil and gas facilities. According to Burby (1998), "a mitigation plan is a statement of intent. It states aspirations, principles of action, and specific courses of action to achieve those aspirations." It is developed through a systematic process involving a representation of business officials, both strategic management and security professionals. Making this type of a plan rests on data like that presented above and can serve several purposes. Among these are:

- The planning process enables the business to consider physical security in a systematic and comprehensive manner that can be tied back to business decisions such as budgets, human resources needs, etc.

- The process demonstrates the connection between physical security and proposed business policies or programs.

- The process educates decision-makers and staff inside the organization.

- The process can serve to coordinate multiple issues, goals, policies and programs within the organization.

- Adopting this approach brings a number of useful, mature methods into use by the organization.

The mitigation planning process includes the following steps:

- The organization develops the planning intelligence needed to serve as the basis for the plan (like that presented above). This intelligence acts as the basis for the plan and serves as the foundation for the plan.

- The organization sets achievable goals and objectives. This describes the plans and benchmarks for achieving desired outcomes derived from the first step. For example one goal might be target programs/policies for reducing vulnerability. This goal might be achieved by increases staff survivability or decreasing the time needed to return to full production after an attack—this can be articulated as a desire to increase organizational resilience in the wake of an attack.

- The organization must then adopt goals and policies which lay out the actions required to achieve the plans objectives. This step is the road map for accomplishing the second step. It acts as the connective tissue between the business plan and the security plan.

- Finally the organization must conduct longitudinal monitoring, evaluation, and revision. This part of the plan establishes how the effectiveness of the plan will be determined,

how the plan will be executed and implemented. Finally, it describes how the plan will adapt to changing circumstances.

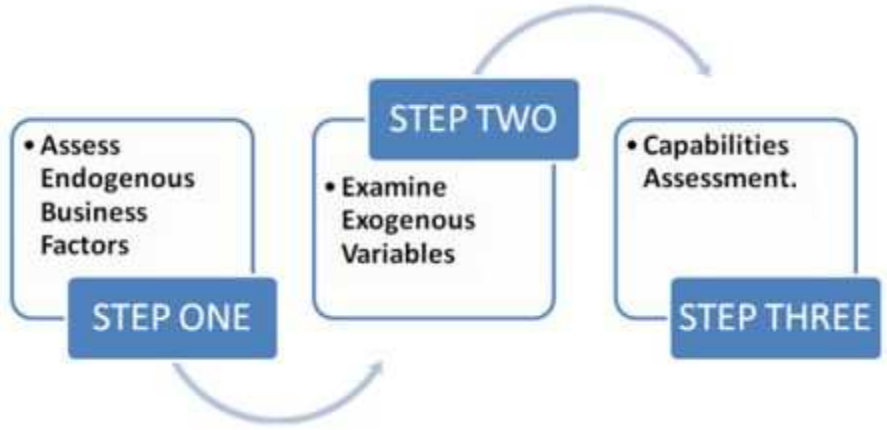
Developing Planning Intelligence

The critical problem in developing planning intelligence was artfully expressed by former U.S. Defense Secretary Donald Rumsfeld in a press briefing in 2002 (Rumsfeld 2002):

“The challenge for us is that we know there are known known’s. There are things we know we know. We also know there are known unknowns. That is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know."

A key problem for decision-makers in envisioning the future is to reduce the size of the unknown unknowns. In order to do this, the envisioning the future process advocate the use of futures forecasting techniques such as scenario designs and in the process adding relevance to the analysis. In performing these analytical techniques, it is necessary to cast the widest possible net in receiving input. It is necessary to look outside normal organizational constraints to find and assess the effect of the unknown unknowns.

Figure Five: Scenario Design



In scenario design, the traditional three step process is readily adaptable to the problem of physical security planning (see Figure Five above). In the first step, endogenous business factors are assessed. Factors here are well within the control of the business or organization assessing the threat. In this case, the threats may come from competitors or be business management decisions that reflect budgets, time schedules or staffing levels.

The second step in scenario design becomes more problematic when physical security is considered. The normal second step is to examine exogenous variables. That is those things that occur outside the scope of the organization. Here traditional scenario approaches identify a limited number of variables that may affect the organization yet are not within the organizations control. Examples of these kinds of variables are world petroleum demand, religious fervor, or social change. It is our opinion that the vast majority of “unknown unknowns” reside in this step of the planning process.

The process of developing planning intelligence for this step is a challenging multifaceted and continuous process. Generating inputs to scenario design for this step should include techniques normally found in hazard mitigation planning. The hazard assessment is one useful technique.

The hazard assessment can be undertaken in a variety of different ways with varying degrees of specificity. At the least specific level hazard identification locates hazardous areas or areas where multiple hazards occur, typically without assessing the probability of the hazard being manifested. If the analysis assumes the hazards occur regardless of probability, the hazard identification process can be helpful in producing a worst-case scenario.

An additional level of input is found in the vulnerability assessment. This kind of assessment estimates the number of people or business facilities exposed to potential hazards. It provides an estimate of the dollar value for a number of people potentially impacted should the hazard the manifested. Here again the probability of the hazard manifesting itself is not considered.

The most detailed kind of hazard assessment is the risk assessment which estimates the probable degree of injury and property damage in a given area over a specific time interval should the hazard occur. A problem with risk assessments is that they can become tendentious in the event of arguments over the probabilities or they can be used as a way to inadvertently screening out possible but not likely hazards.

The final step in scenario design should be an assessment of the current capabilities of the organization. It is important to assess how much ability currently exists in the organization and the capacity to respond. This will identify areas in which the resilience of the organization in response to a physical security problem can be enhanced and the organization becomes more resilient. This was demonstrated in World War II to geostrategic level by the development of floating reserves that enabled the uninterrupted flow of oil to Allied fighting forces throughout the war. The system was resilient and could adapt to different circumstances.

The challenge of scenario development is how to effectively marshal information and methods. These will enable assessments to be performed and help generate analyses that support the incorporation of nontraditional methods/data. This then is applied to the various industrial means that will be used to find, extract, transport, refine and deliver the oil and gas products to the final market.

The range of origination/extraction points, the multiple modes of transportation necessary to service those points, the varied facilities needed to accomplish the processing and subsequent transport/transfer of the end products and the delivery of the final product to the end market, all need to be assessed as to their common and unique risk factors.

Conclusion

This paper suggests that techniques found in traditional hazard mitigation planning processes can be useful in designing physical security planning processes for oil and gas production and transmission facilities. These facilities have traditionally been subjected to violent disruption and attacks. Whether the attacks were directed by organized labor, terrorist organizations, or state actors intent on achieving a strategic goal, petroleum facilities have been both vulnerable to attack and considered desirable targets.

Critically important in assessing potential threats to these facilities is the need to undertake a fully integrated physical security planning process that works with business planning cycles. These are used in conjunction to develop plans that wholly support and reflect the physical security situation. To that end physical security planning and mitigation planning must consider factors and variables that are geostrategic in nature and fall outside some of the normal objectives of the traditional hazard mitigation planning approach.

To achieve this approach it is necessary to invest heavily in the development of intelligence that supports these kinds of plans. This kind of intelligence incorporates scenarios and other futures

methodologies. There are however unique characteristics found in physical security planning that are outside the normal kinds of business future scenarios planning. To fully embrace these plans it is necessary to effectively articulate the problem and to search outside normal organizational structures to develop effective planning processes for terrorism threats.

About the Author

James David Ballard, Ph.D. is Associate Professor of Sociology at California State University, Northridge. Fred C. Dilger, Ph.D. is a Principal at Black Mountain Research, in Henderson, Nevada.

References

Adams, N. 2003. *Terrorism and Oil.* Tulsa, OK: The PennWell Corporation.

Alnasrawi, A. 1994. *The Economy of Iraq: Oil, Wars, Destruction of Development and Prospects*. Westport, CT: Greenwood Press.

Ballard, J. D. (2002a). "Shelter-in-Place: The necessary logic behind high-level nuclear waste security." White paper submitted to the State of Nevada. Carson City, Nevada.

Ballard, J.D. (2002b). “Asymmetrical Sabotage Tactics, Nuclear Facilities/Materials and Vulnerability Analysis.” Paper presented at NUMAT Conference, Salzburg Austria. Download Date August 5, 2007. Available online at http://www.numat.at/

Blankenship, J. 2002. “International Standard for Design Basis Threat (DBT).” Paper presented at NUMAT Conference, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/

Bridgeland, T. and A, Morgan. 2003. *Tunnelmaster and Arsonist of the Great War: The Norton-Griffiths Story.* South Yorkshire: Pen and Sword Books.

Chaliand, G. and A. Blin. *The History of Terrorism: From Antiquity to Al Qaeda.* Berkeley: University of California Press.

Glenn, J. C. and T. J. Gordon. 1999. “Futures Research Methodology, 2nd edition.” Published by the American Council for the United Nations University: The Millennium Project. Available in CD format at www.acunu.org.

Halstead, R., Ballard, J. D., & Dilger, F. (2001). “Nuclear Waste Transportation Terrorism and Sabotage: Critical Issues.” Paper presented at the 13th annual symposium on packaging and transportation of radioactive materials, PATRAM 2001Conference. Chicago, IL: September 2001.

Hamilton, J. D. 1983. “Oil and the Macroeconomy since WW II.” *Journal of Political Economy* 91, No. 2, 228-248.

Hiro, D. 1991. *The Longest War: The Iran-Iraq Military Conflict*. London: Routledge.

Institute for the Analysis of Global Security. June 2007. *Energy Security.* Download date: July 7, 2007. Available online at www.iags.org .

IAEA (International Atomic Energy Agency). 2007. “Requirements for Physical Protection Against Sabotage of Nuclear Facilities and Nuclear Material During Use and Storage.” Download date: August 5, 2007. Available online at http://www.iaea.org/

Kalicki, J. H. and D. L. Goldwyn. 2005. *Energy and Security: Toward a New Foreign Policy Strategy.* Washington, DC: Woodrow Wilson Center Press.

Makarenko, T. 2003 (May/June). “Terrorist Threat to Energy Infrastructure Increases.” *Jane’s Intelligence Review*. Download date July 28, 2007. Available online at http://www.ciaonet.org/wps/mat04/mat04.pdf

Mansfeld, Y. 1999. “Cycles of War, Terror, and Peace: Determinants of the Israeli Tourism Industry.” *Journal of Travel Research* 38, No. 1, 30-36.

Ness , L. 2006: *Securing Utility and Energy Infrastructures.* Hoboken, NJ: John Wiley and Sons.

Perry, G. L. “The War on Terrorism, the World Oil Market and the U.S. Economy.” Published by the Brookings Institute. Download date July 28, 2007. Available online at http://www.brook.edu.

Santiago , M. I. 2006. *The Ecology of Oil: Environment, Labor, and the Mexican Revolution, 1990-1938.* New York: Cambridge University Press.

Sampson, A. 1975. *The Seven Sisters: The Great Oil Companies and the World They Made.* London: Hodder and Stoughton.

Threat Reduction Limited. May 2007. *Oil and Gas Industry Terrorism Monitor.* Download: July 7, 2007. Available online at www.ogi-tm.com.

Time Magazine. Oct. 8, 1951. “Seizure of Abadan.” Download date: August 5, 2007. Available online at www.time.com.

Toffler, A. *The Third Wave.* New York: Random House.

USNRC (United States Nuclear Regulatory Commission). 2007. “Design Basis Threat.” Download date August 5, 2007. Available online at http://www.nrc.gov/

Willis, H. H., A. R. Morral, T. K. Kelly and J. J. Medby. 2005. *Estimating Terrorism Risk.* Santa Monica: Rand Corporation.

Yergin, D. (1992). *The Prize: The Epic Quest for Oil, Money & Power*. New York, NY: Free Press.

Yetiv, S. 2004. *Crude Awakenings: Global Oil Security and American Foreign Policy.* Ithaca, NY: Cornell University Press.